HEALTH AFFAIRS

TRICARE
TRICARE
Management
Activity

HIPAA Security Special Topics

HIPAA Training: Summer Session

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

Agenda

- HIPAA Security Resources
- Biomedical Devices
- Virtual Private Networks

HIPAA Security Resources

Agenda

- HIPAA Security Poster Campaign
- Privacy Office Web Site
- Risk Information Management Resource (RIMR)

HIPAA Security Resources

Objectives

- Upon completion of this course you will be able to:
  - Identify available resources to aide in Security Awareness
  - Identify available training briefings
  - Describe the organization, content, implementation strategy of the HIPAA Security Poster Campaign
  - Identify available resources to aide in implementation of HIPAA Security

HIPAA Security Poster Campaign

HIPAA Security Poster Campaign

Objectives

- Upon completion of this module, you should be able to:
  - Describe the purpose and origin of the poster campaign
  - Identify the content of the posters
  - Plan how to integrate the posters into your existing security awareness program

HIPAA Security Poster Campaign

Background

- Developed by HIPAA Security IPT Training and Education Subcommittee
- Purpose:
  - Aide in increasing awareness of good security practices
  - Target audience is information system users
  - Designed as a long term campaign (1 for each month of the year)
  - Designed to integrate into other existing training and awareness programs

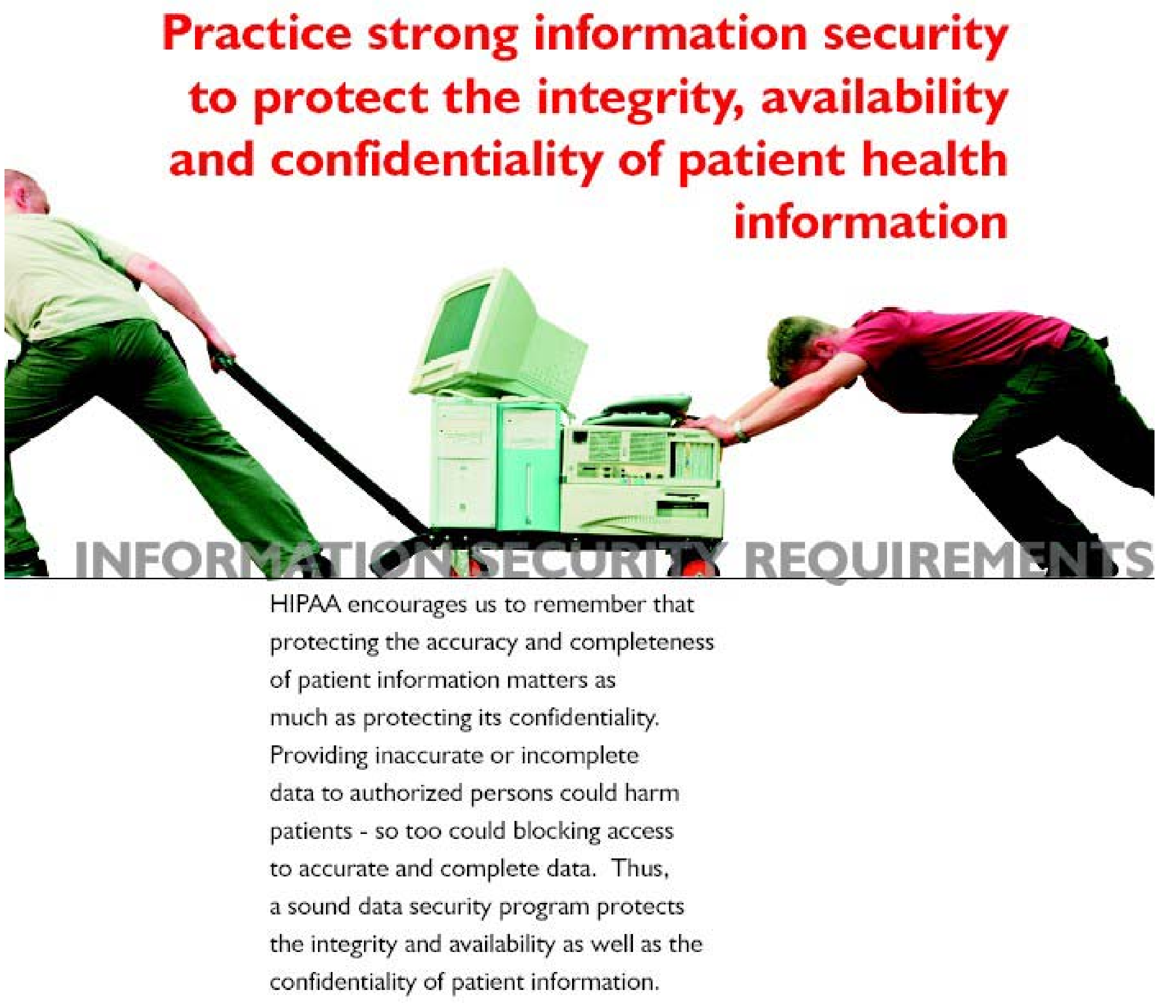
HIPAA Security Poster Campaign

Content

- Posters grouped into three themes Confidentiality, Integrity, and Availability, with one comprehensive poster that combines all three
- Contemporary design to catch the eye
- One color for each theme
- Each poster has the theme, a topic, slogan and text

HIPAA Security Poster Campaign

Poster Samples (1 of 4)



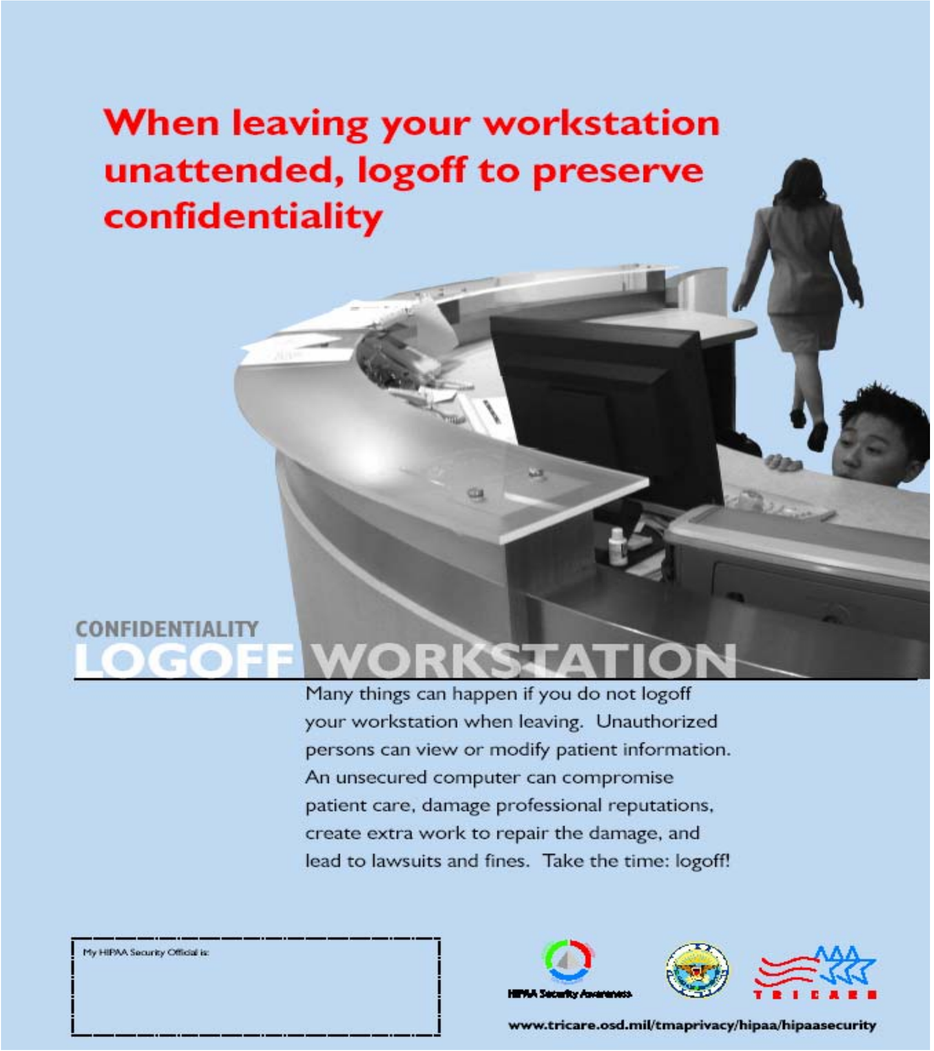
Practice strong information security to protect the integrity, availability and confidentiality of patient health information

INFORMATION SECURITY REQUIREMENTS

HIPAA encourages us to remember that protecting the accuracy and completeness of patient information matters as much as protecting its confidentiality. Providing inaccurate or incomplete data to authorized persons could harm patients - so too could blocking access to accurate and complete data. Thus, a sound data security program protects the integrity and availability as well as the confidentiality of patient information.

HIPAA Security Poster Campaign

Poster Samples (2 of 4)



When leaving your workstation unattended, logoff to preserve confidentiality

CONFIDENTIALITY

LOGOFF WORKSTATION

Many things can happen if you do not logoff your workstation when leaving. Unauthorized persons can view or modify patient information. An unsecured computer can compromise patient care, damage professional reputations, create extra work to repair the damage, and lead to lawsuits and fines. Take the time: logoff!

My HIPAA Security Official is:

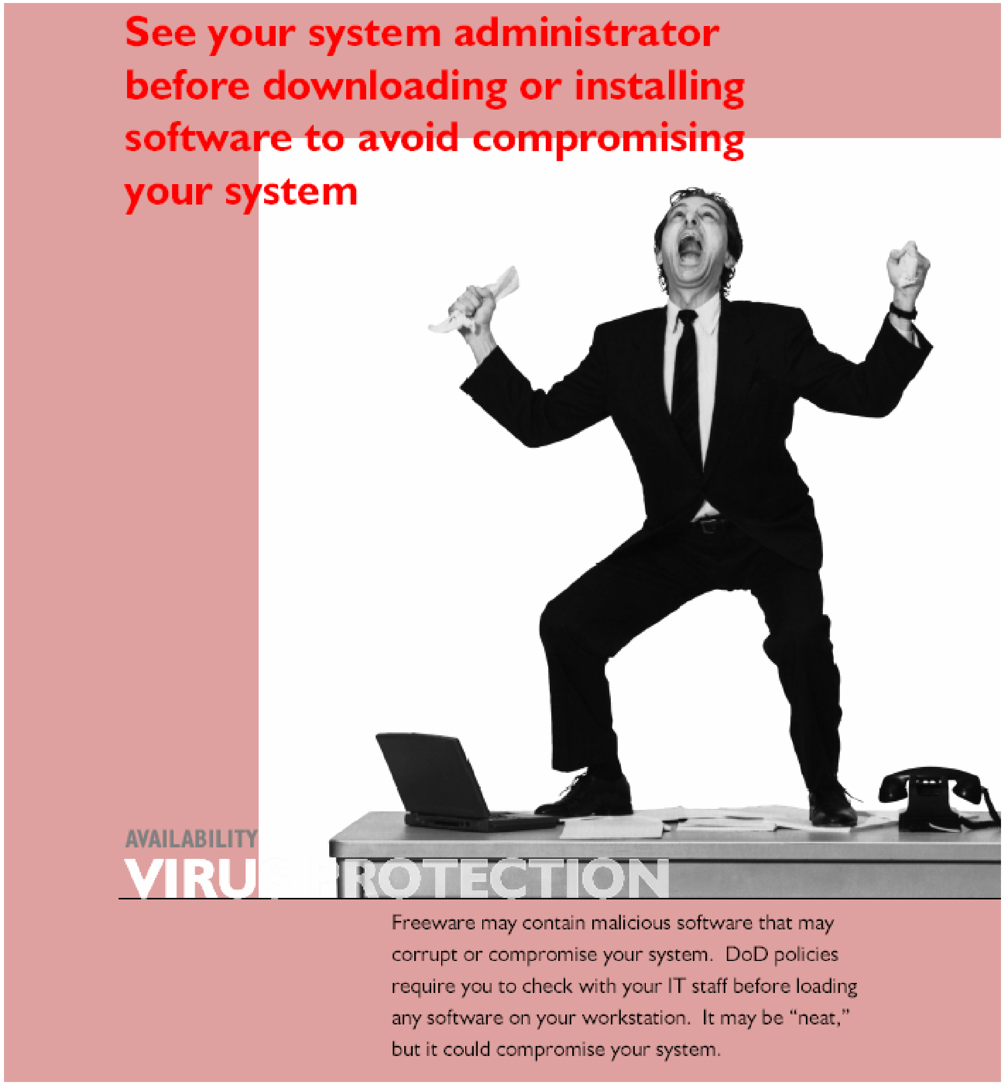
HIPAA Security Awareness

TRICARE

www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

HIPAA Security Poster Campaign

Poster Samples (3 of 4)



See your system administrator before downloading or installing software to avoid compromising your system

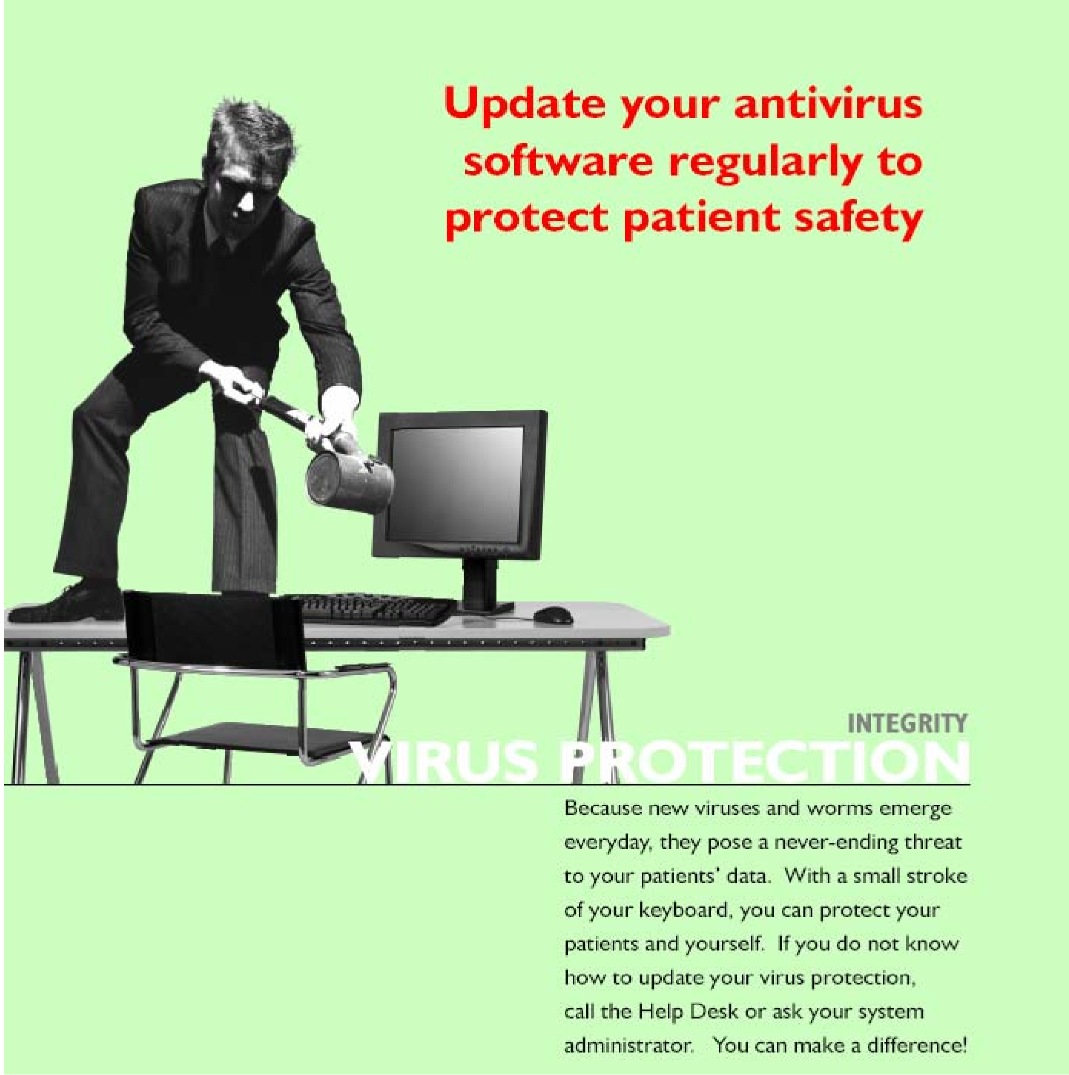
AVAILABILITY

VIRUS PROTECTION

Freeware may contain malicious software that may corrupt or compromise your system. DoD policies require you to check with your IT staff before loading any software on your workstation. It may be "neat," but it could compromise your system.

HIPAA Security Poster Campaign

Poster Samples (4 of 4)



Update your antivirus software regularly to protect patient safety

INTEGRITY

VIRUS PROTECTION

Because new viruses and worms emerge everyday, they pose a never-ending threat to your patients' data. With a small stroke of your keyboard, you can protect your patients and yourself. If you do not know how to update your virus protection, call the Help Desk or ask your system administrator. You can make a difference!

HIPAA Security Poster Campaign

Distribution

- Posters are currently being printed
- Distributed once a month starting with comprehensive poster
- Distribution coordinated with related information via e-newsletter
- 3 copies of each poster to each MTF
  - Limited number of additional posters available on request
- Mailed to each MTF’s Privacy or Security Officer

HIPAA Security Poster Campaign

How to Integrate Posters

- Review elements of your current programs and or resources to:
  - Determine which elements can be used to promote awareness of the posters (e.g., existing monthly staff newsletters)
  - Use posters and related material to support other programs that are related to either security or HIPAA
  - Build on poster themes and topics in your own awareness campaign
- Post in elevator lobbies and other high traffic areas

HIPAA Security Poster Campaign

Lesson Summary

- You should now be able to:
  - Describe the purpose and origin of the poster campaign
  - Identify the content of the posters
  - Plan how to integrate the posters into your existing security awareness program

TMA HIPAA Security Web Site

TMA HIPAA Security Web Site

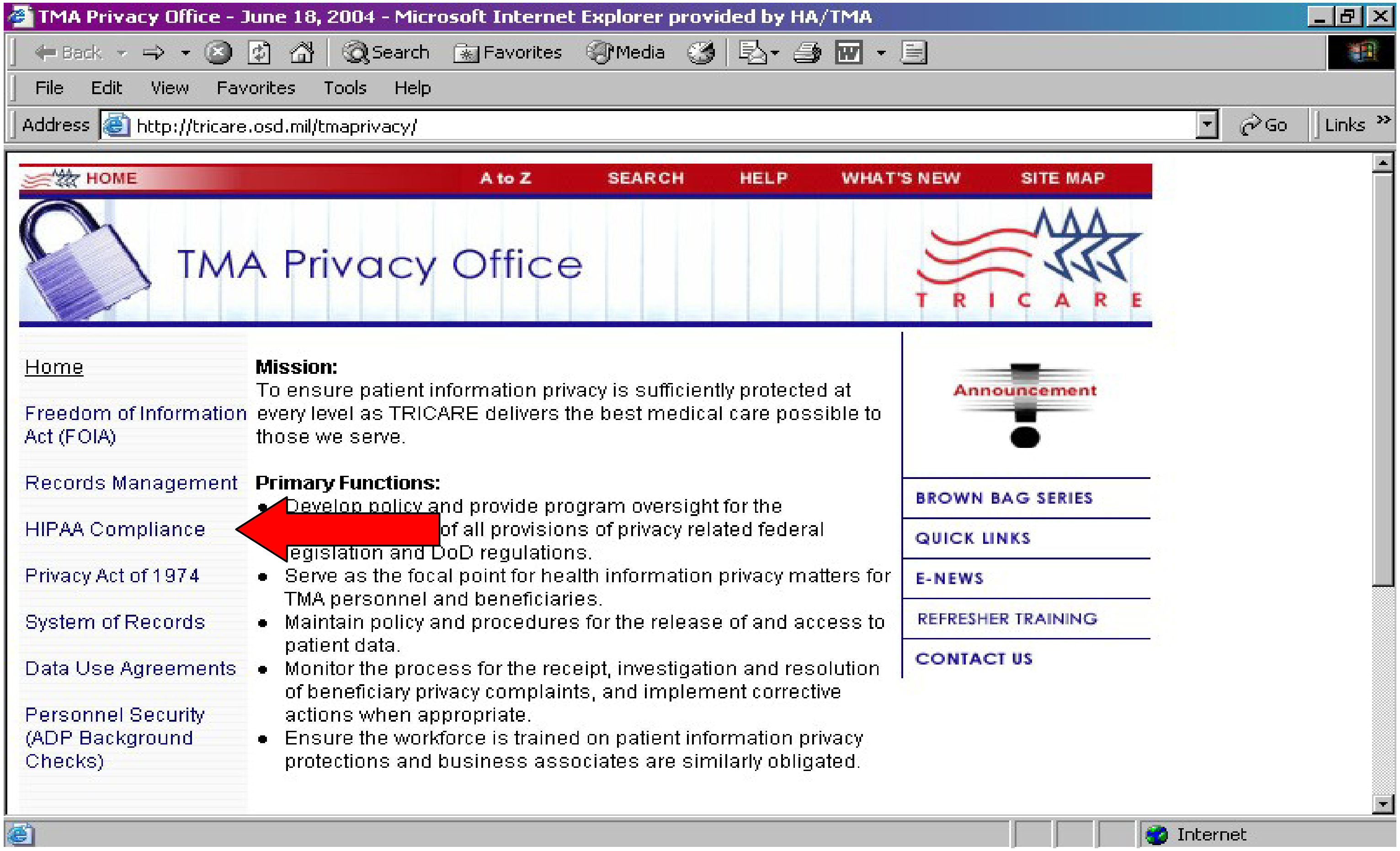
Objectives

- Upon completion of this module, you should be able to:
  - Identify what resources are available on the web site
  - Locate the resources on the web site
  - Subscribe to the TMA Privacy Office e-news

TMA HIPAA Security Web Site

Where is it? (1 of 3)

http://tricare.osd.mil/tmaprivacy/



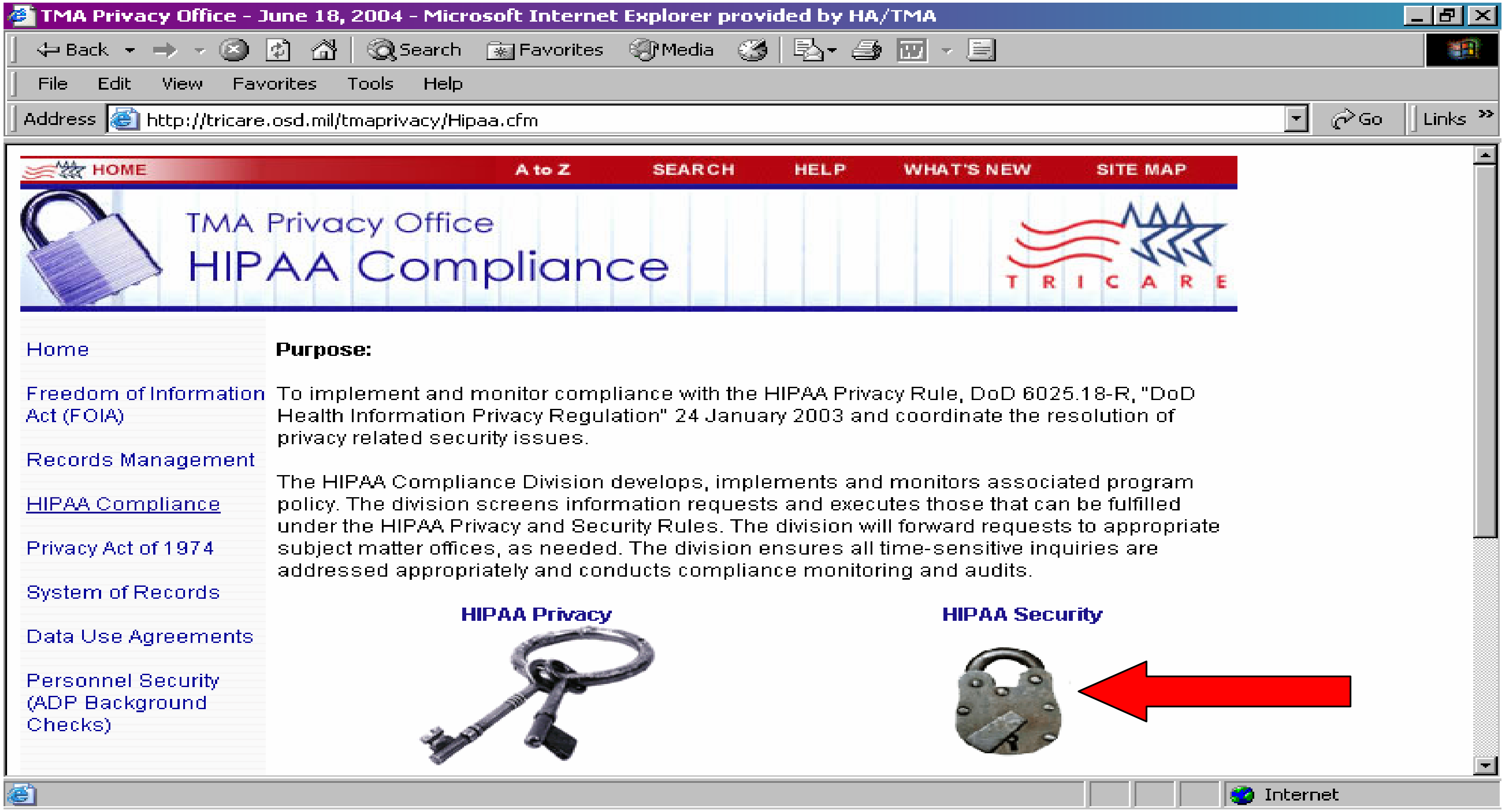
Mission:
To ensure patient information privacy is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Primary Functions:

- Develop policy and provide program oversight for the of all provisions of privacy related federal legislation and DoD regulations.
- Serve as the focal point for health information privacy matters for TMA personnel and beneficiaries.
- Maintain policy and procedures for the release of and access to patient data.
- Monitor the process for the receipt, investigation and resolution of beneficiary privacy complaints, and implement corrective actions when appropriate.
- Ensure the workforce is trained on patient information privacy protections and business associates are similarly obligated.

TMA HIPAA Security Web Site

Where is it? (2 of 3)



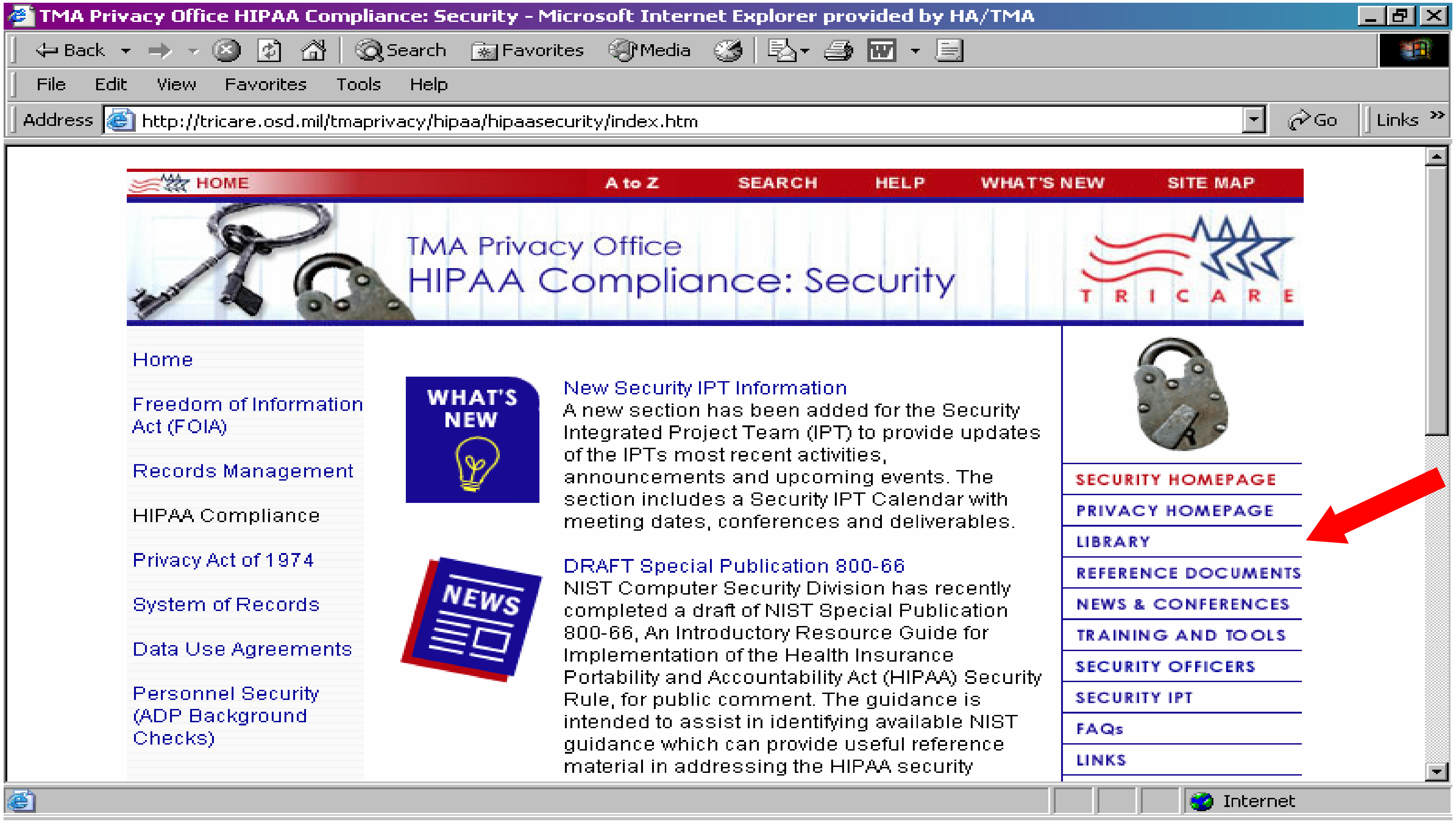
Purpose:

To implement and monitor compliance with the HIPAA Privacy Rule, DoD 6025.18-R, "DoD Health Information Privacy Regulation" 24 January 2003 and coordinate the resolution of privacy related security issues.

The HIPAA Compliance Division develops, implements and monitors associated program policy. The division screens information requests and executes those that can be fulfilled under the HIPAA Privacy and Security Rules. The division will forward requests to appropriate subject matter offices, as needed. The division ensures all time-sensitive inquiries are addressed appropriately and conducts compliance monitoring and audits.

TMA HIPAA Security Web Site

Where is it? (3 of 3)



New Security IPT Information

A new section has been added for the Security Integrated Project Team (IPT) to provide updates of the IPTs most recent activities, announcements and upcoming events. The section includes a Security IPT Calendar with meeting dates, conferences and deliverables.

DRAFT Special Publication 800-66

NIST Computer Security Division has recently completed a draft of NIST Special Publication 800-66, An Introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, for public comment. The guidance is intended to assist in identifying available NIST guidance which can provide useful reference material in addressing the HIPAA security

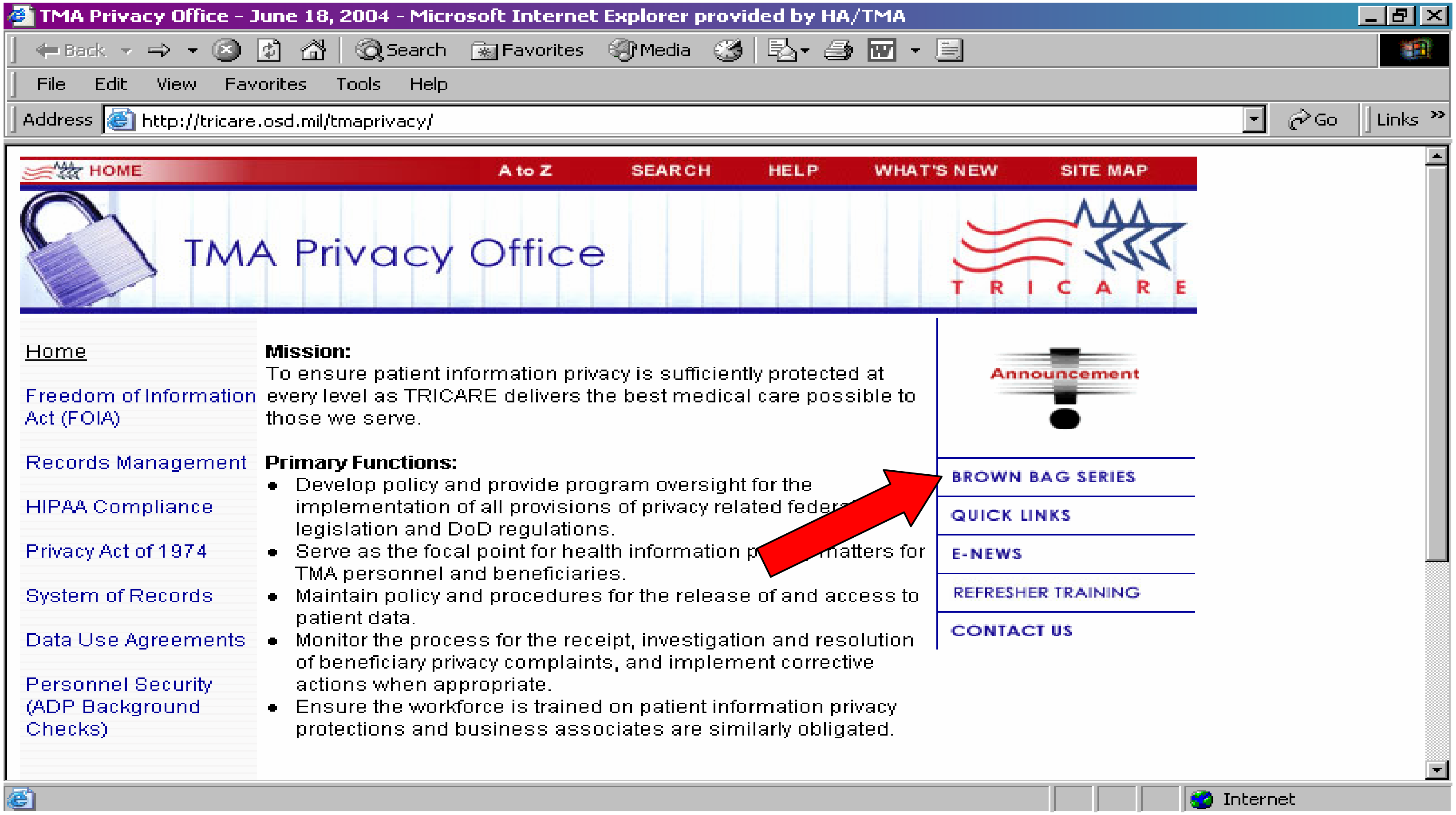
TMA HIPAA Security Web Site

What's in the Library

- The Library contains:
  - HIPAA Security Overview and 25 other related information papers
  - Briefings
  - Security Officer appointment letters and responsibilities

TMA HIPAA Security Web Site

Brown Bag Series (1 of 3)



Home

Freedom of Information Act (FOIA)

Records Management

HIPAA Compliance

Privacy Act of 1974

System of Records

Data Use Agreements

Personnel Security (ADP Background Checks)

Mission:
To ensure patient information privacy is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Primary Functions:

- Develop policy and provide program oversight for the implementation of all provisions of privacy related federa[illegible] legislation and DoD regulations.
- Serve as the focal point for health information p[illegible] matters for TMA personnel and beneficiaries.
- Maintain policy and procedures for the release of and access to patient data.
- Monitor the process for the receipt, investigation and resolution of beneficiary privacy complaints, and implement corrective actions when appropriate.
- Ensure the workforce is trained on patient information privacy protections and business associates are similarly obligated.

Announcement

BROWN BAG SERIES

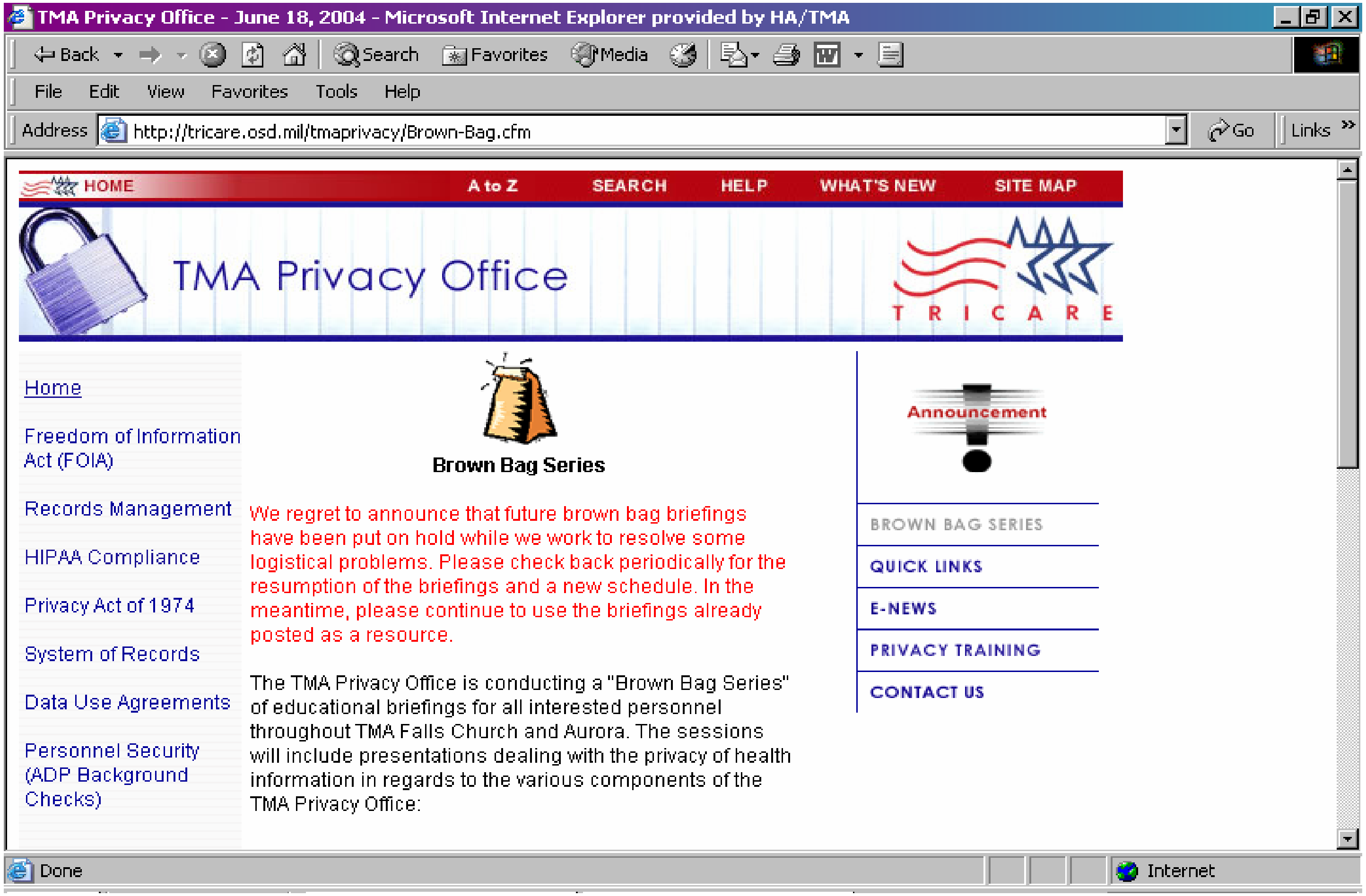
QUICK LINKS

E-NEWS

REFRESHER TRAINING

CONTACT US

TMA HIPAA Security Web Site
Brown Bag Series (2 of 3)



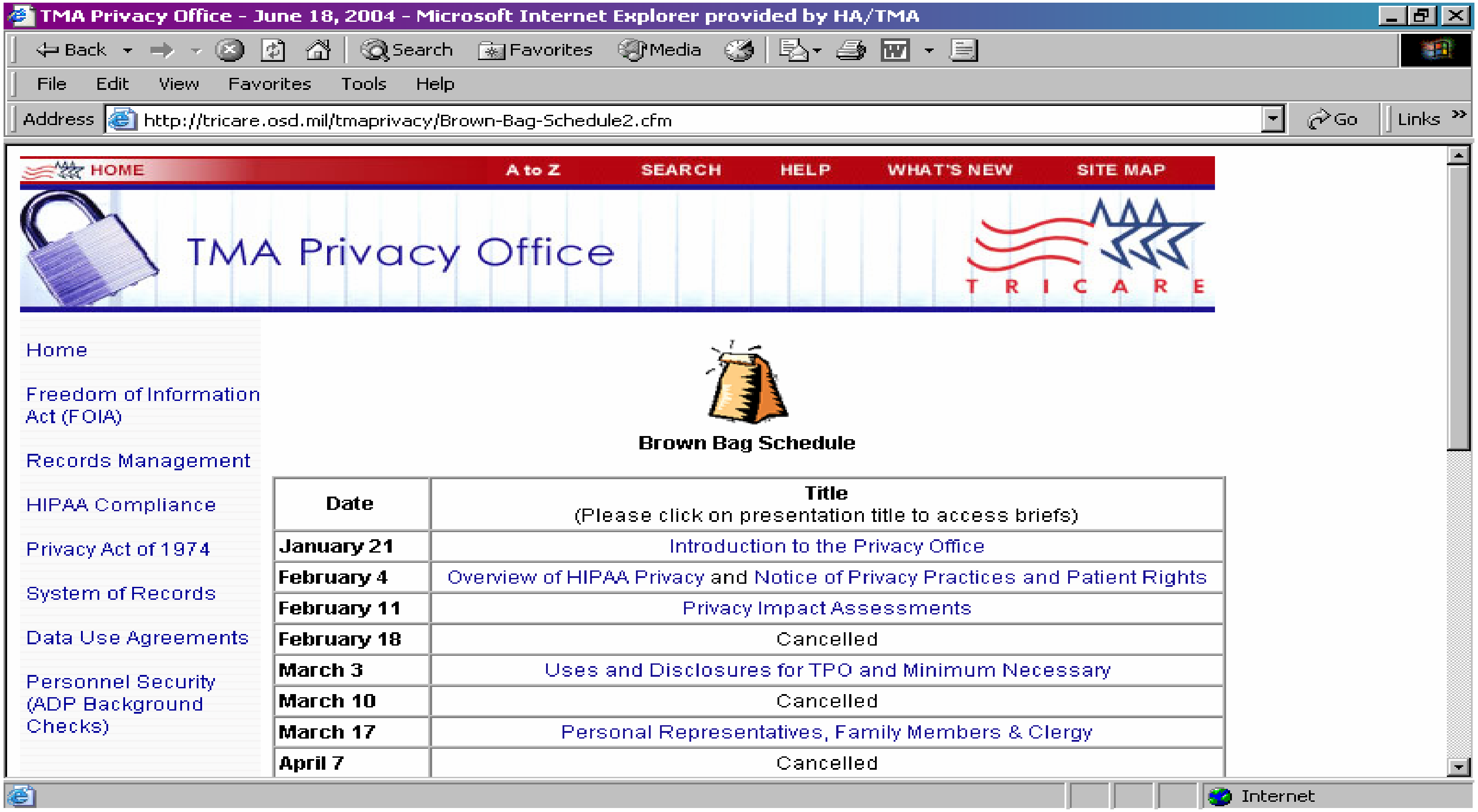
Brown Bag Series

We regret to announce that future brown bag briefings have been put on hold while we work to resolve some logistical problems. Please check back periodically for the resumption of the briefings and a new schedule. In the meantime, please continue to use the briefings already posted as a resource.

The TMA Privacy Office is conducting a "Brown Bag Series" of educational briefings for all interested personnel throughout TMA Falls Church and Aurora. The sessions will include presentations dealing with the privacy of health information in regards to the various components of the TMA Privacy Office:

TMA HIPAA Security Web Site

Brown Bag Series (3 of 3)

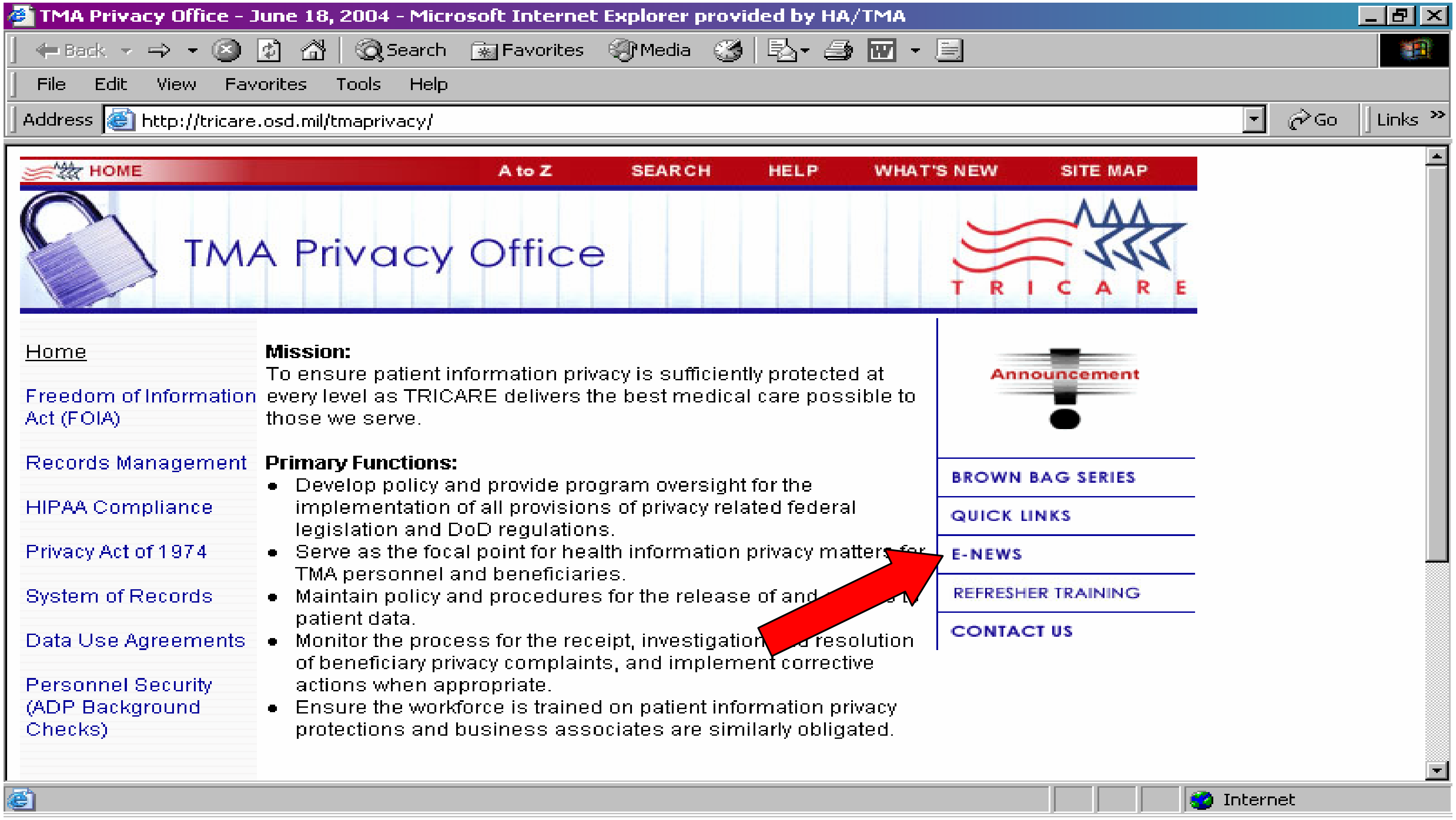


Brown Bag Schedule

Date	Title (Please click on presentation title to access briefs)
January 21	Introduction to the Privacy Office
February 4	Overview of HIPAA Privacy and Notice of Privacy Practices and Patient Rights
February 11	Privacy Impact Assessments
February 18	Cancelled
March 3	Uses and Disclosures for TPO and Minimum Necessary
March 10	Cancelled
March 17	Personal Representatives, Family Members & Clergy
April 7	Cancelled

TMA HIPAA Security Web Site

E-NEWS (1 of 2)



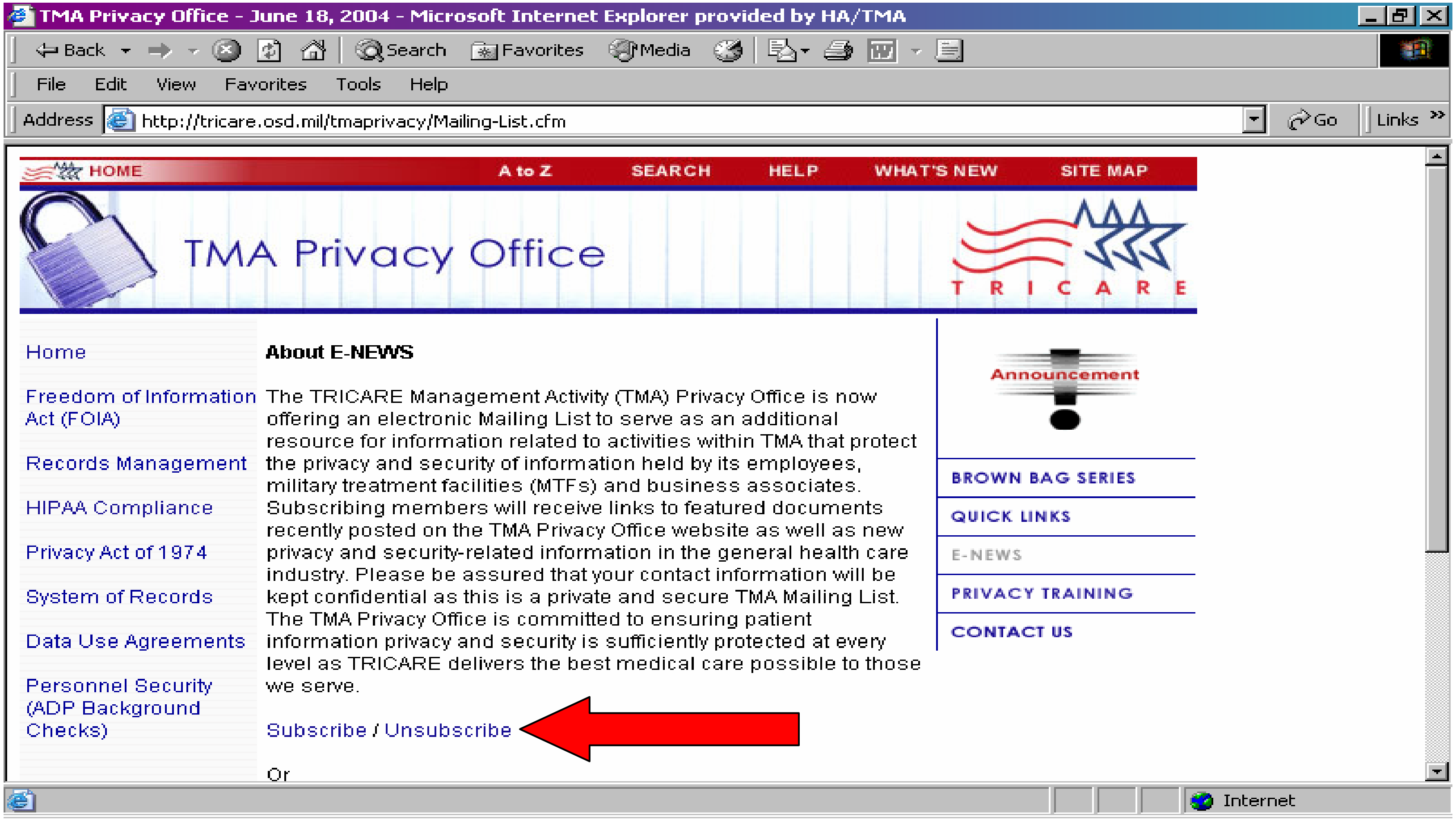
Mission:
To ensure patient information privacy is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Primary Functions:

- Develop policy and provide program oversight for the implementation of all provisions of privacy related federal legislation and DoD regulations.
- Serve as the focal point for health information privacy matters for TMA personnel and beneficiaries.
- Maintain policy and procedures for the release of and [illegible] patient data.
- Monitor the process for the receipt, investigation [illegible] resolution of beneficiary privacy complaints, and implement corrective actions when appropriate.
- Ensure the workforce is trained on patient information privacy protections and business associates are similarly obligated.

TMA HIPAA Security Web Site

E-NEWS (2 of 2)



About E-NEWS

The TRICARE Management Activity (TMA) Privacy Office is now offering an electronic Mailing List to serve as an additional resource for information related to activities within TMA that protect the privacy and security of information held by its employees, military treatment facilities (MTFs) and business associates. Subscribing members will receive links to featured documents recently posted on the TMA Privacy Office website as well as new privacy and security-related information in the general health care industry. Please be assured that your contact information will be kept confidential as this is a private and secure TMA Mailing List. The TMA Privacy Office is committed to ensuring patient information privacy and security is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Subscribe / Unsubscribe

Or

TMA HIPAA Security Web Site

Lesson Summary

- You should now be able to:
  - Identify what resources are available on the web site
  - Locate the resources on the web site
  - Subscribe to the TMA Privacy Office E-NEWS

Risk Information Management Resource (RIMR)

RIMR

Objectives

- Upon completion of this module, you should be able to:
  - Locate RIMR
  - Identify resources on RIMR

What is RIMR? (1 of 2)

- Web portal to provides access to:
  - IA resources (policies, case studies, white papers)
  - P3WG HIPAA Privacy and Security Reports
  - OCTAVE (including methodology, automated tool, risk database and support center)
- Database
  - Stores completed risk assessments
  - Provides aggregate reports
  - Can be used to research common vulnerabilities
  - Trend analysis
  - Supports enterprise wide problem solving and mitigation
  - Justification for funding initiatives

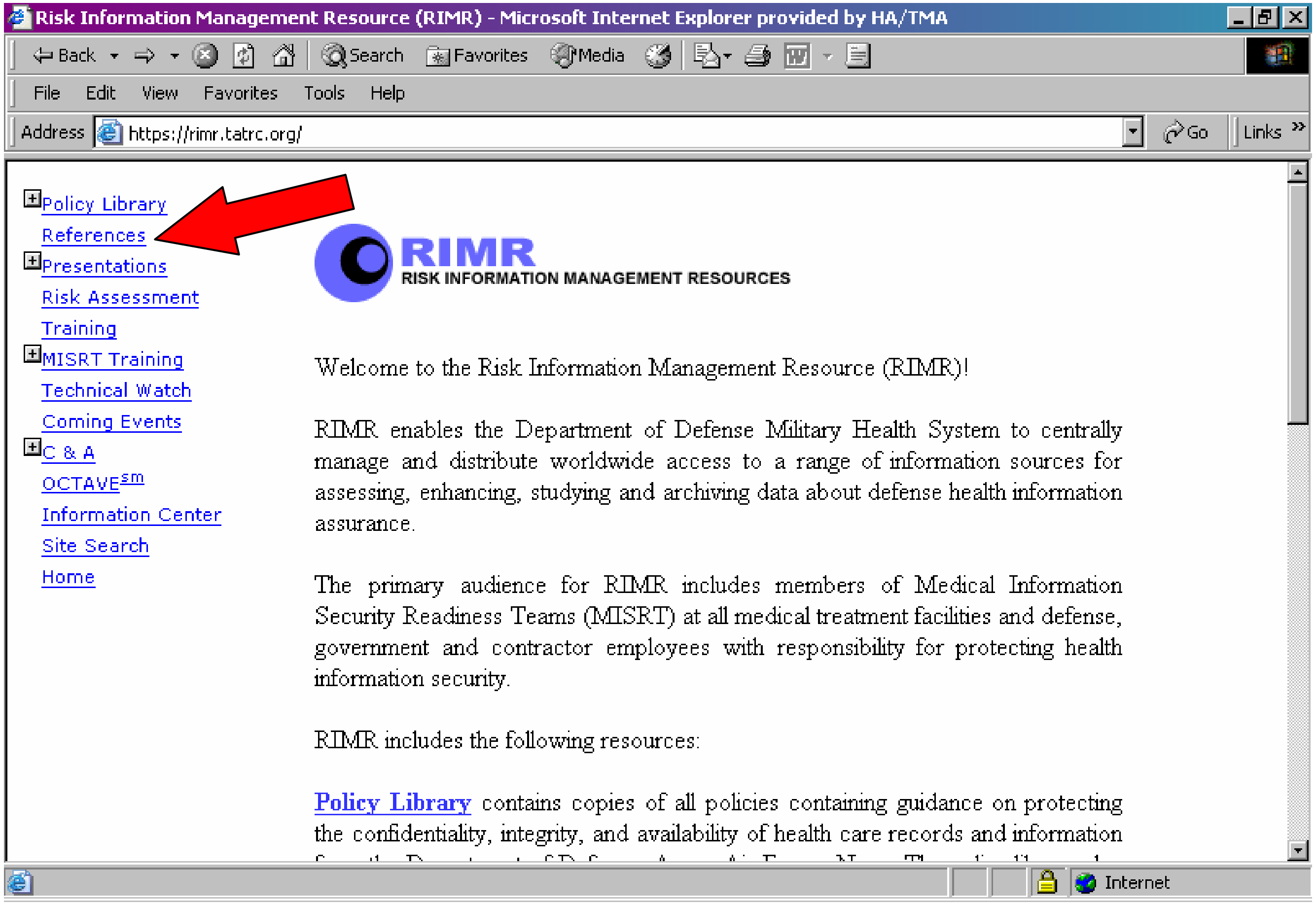
What is RIMR? (2 of 2)

- Congressionally funded through Defense Health Information Assurance Program (DHIAP)
- Currently located at Ft. Detrick
- DoD owned – not vender owned
- Developers
  - Advanced Technology Institute, Charleston SC
  - KRM Associates, Inc, Shepherdstown WV
  - Software Engineering Institute at Carnegie Melon (CERT), Pittsburgh PA

RIMR

Where is RIMR?

https://rimr.tatrc.org



Policy Library
References
Presentations
Risk Assessment
Training
MISRT Training
Technical Watch
Coming Events
C & A
OCTAVE^{sm}
Information Center
Site Search
Home

RIMR
RISK INFORMATION MANAGEMENT RESOURCES

Welcome to the Risk Information Management Resource (RIMR)!

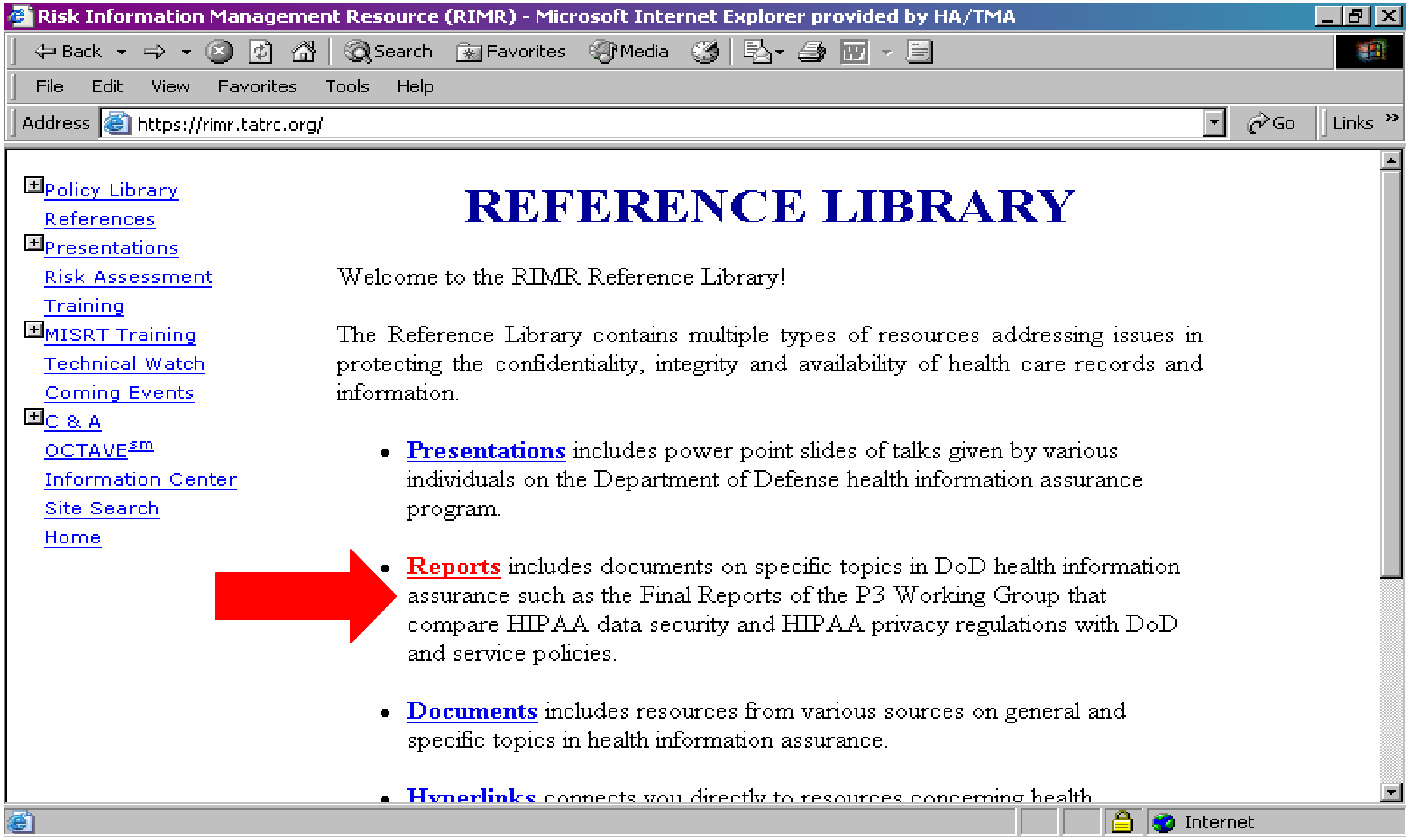
RIMR enables the Department of Defense Military Health System to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance.

The primary audience for RIMR includes members of Medical Information Security Readiness Teams (MISRT) at all medical treatment facilities and defense, government and contractor employees with responsibility for protecting health information security.

RIMR includes the following resources:

Policy Library contains copies of all policies containing guidance on protecting the confidentiality, integrity, and availability of health care records and information

RIMR
Reference Library



Address: https://rimr.tatrc.org/

REFERENCE LIBRARY

Welcome to the RIMR Reference Library!

The Reference Library contains multiple types of resources addressing issues in protecting the confidentiality, integrity and availability of health care records and information.

- **Presentations** includes power point slides of talks given by various individuals on the Department of Defense health information assurance program.
- **Reports** includes documents on specific topics in DoD health information assurance such as the Final Reports of the P3 Working Group that compare HIPAA data security and HIPAA privacy regulations with DoD and service policies.
- **Documents** includes resources from various sources on general and specific topics in health information assurance.
- **Hyperlinks** connects you directly to resources concerning health

RIMR

P3WG Final Report Background

- DHIAP and the DoD/HA HIPAA Overarching Integrated Process Team (OIPT) sponsored the formation of the interdisciplinary and inter-service Policies, Procedures, and Practices Workgroup
- Compared all pertinent DoD and service level regulations with the HIPAA Data Security Rule
- Identified gaps and discrepancies and made recommendations for changes

P3WG Final Report Content

- Executive summary and methodology
- Chapter for each rule and associated implementation specifications
  - HIPAA wording with plain English explanation
  - All mapped citations
  - Compliance analysis with recommendations
- Analysis of results

RIMR

P3WG Final Report Utilization

- Used at multiple levels
- Guide central policymakers in making revisions
- Critical input includes analysis of results and recommendations
- Use as starting point for MTF local analysis
  - Identifies upper level policies and procedures MTF's should follow
  - Identifies gaps local policies and procedures must fill
- Feed remaining gaps into risk analysis

RIMR

Lesson Summary

- You should now be able to:
  - Locate RIMR
  - Identify resources on RIMR

Summary

- You should now be able to:
  - Identify available resources to aide in Security Awareness
  - Identify available training briefings
  - Describe the organization, content, implementation strategy of the HIPAA Security Poster Campaign
  - Identify available resources to aide in implementation of HIPAA Security

HIPAA Security and Biomedical Devices

Agenda

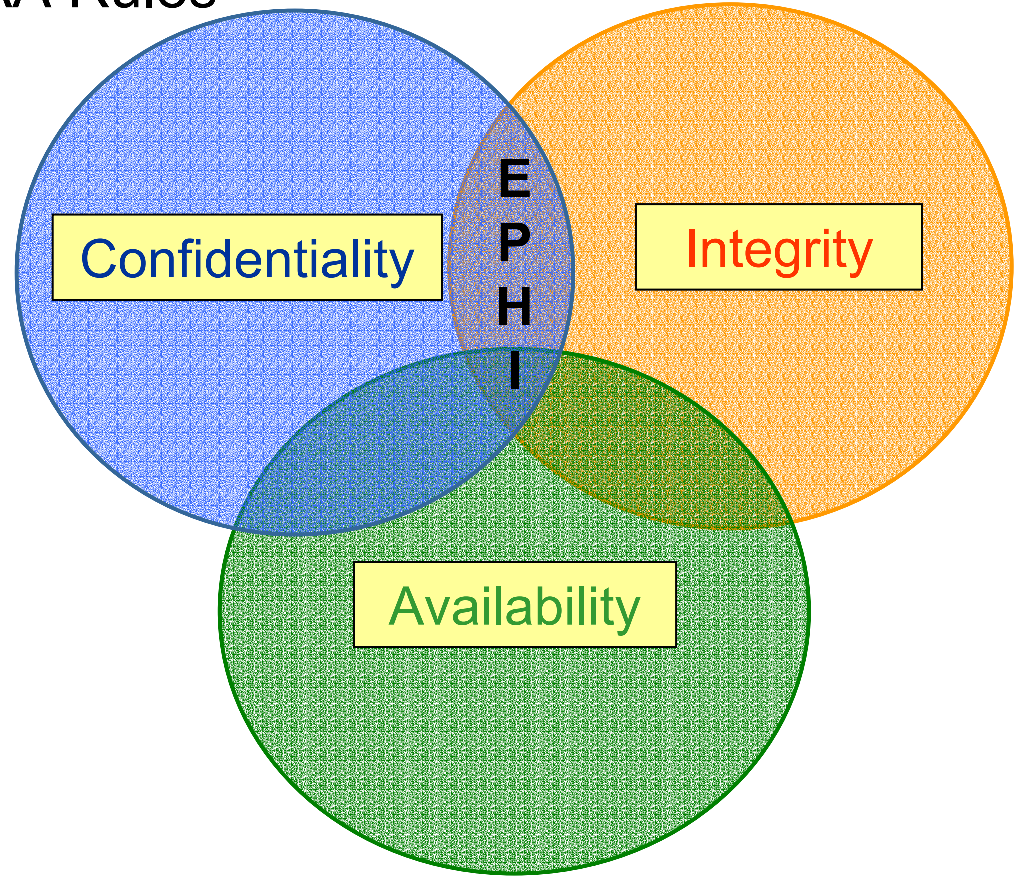
- Relationship between HIPAA and biomedical devices
- Risks presented by the use of biomedical devices
- Possible approaches for minimizing the risks of using biomedical devices

Training Objectives

- Upon completion of this course you should be able to:
  - Describe the relationship between HIPAA security and biomedical devices
  - Detail the risks of using biomedical devices
  - Identify approaches for minimizing these vulnerabilities

HIPAA Security Requirement

- Must protect the confidentiality, integrity, and availability of any electronic health information that is protected under the HIPAA Rules



Where is EPHI found?

- Workstations
- Laptops
- Modems
- Databases
- Digitally recorded voice messages
- Computer-based facsimiles
- Servers
- Applications
- Network connections
- PDAs
- ***Biomedical devices***
- Compact disks
- Floppy diskettes

…..and many more!

HIPAA Security and Biomedical Devices

Biomedical Devices

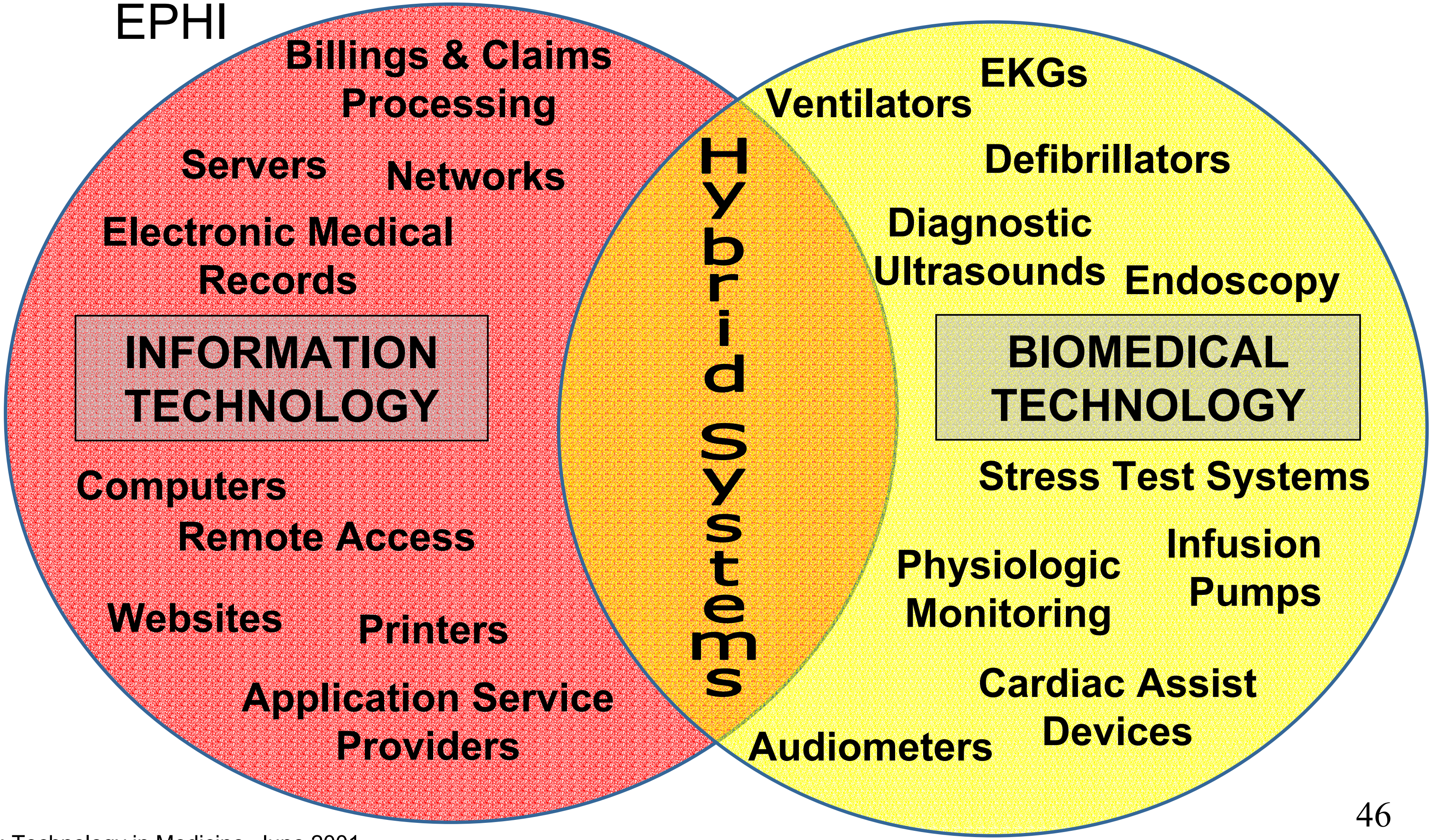
- A biomedical device is defined as “…an instrument which is intended for use in the diagnosis of disease, or other conditions, or in the cure, mitigation, treatment or prevention of disease…” (Food and Drug Administration, 1989)

- Majority of these instruments are highly automated and collect and store health information

HIPAA Security and Biomedical Devices

Systems

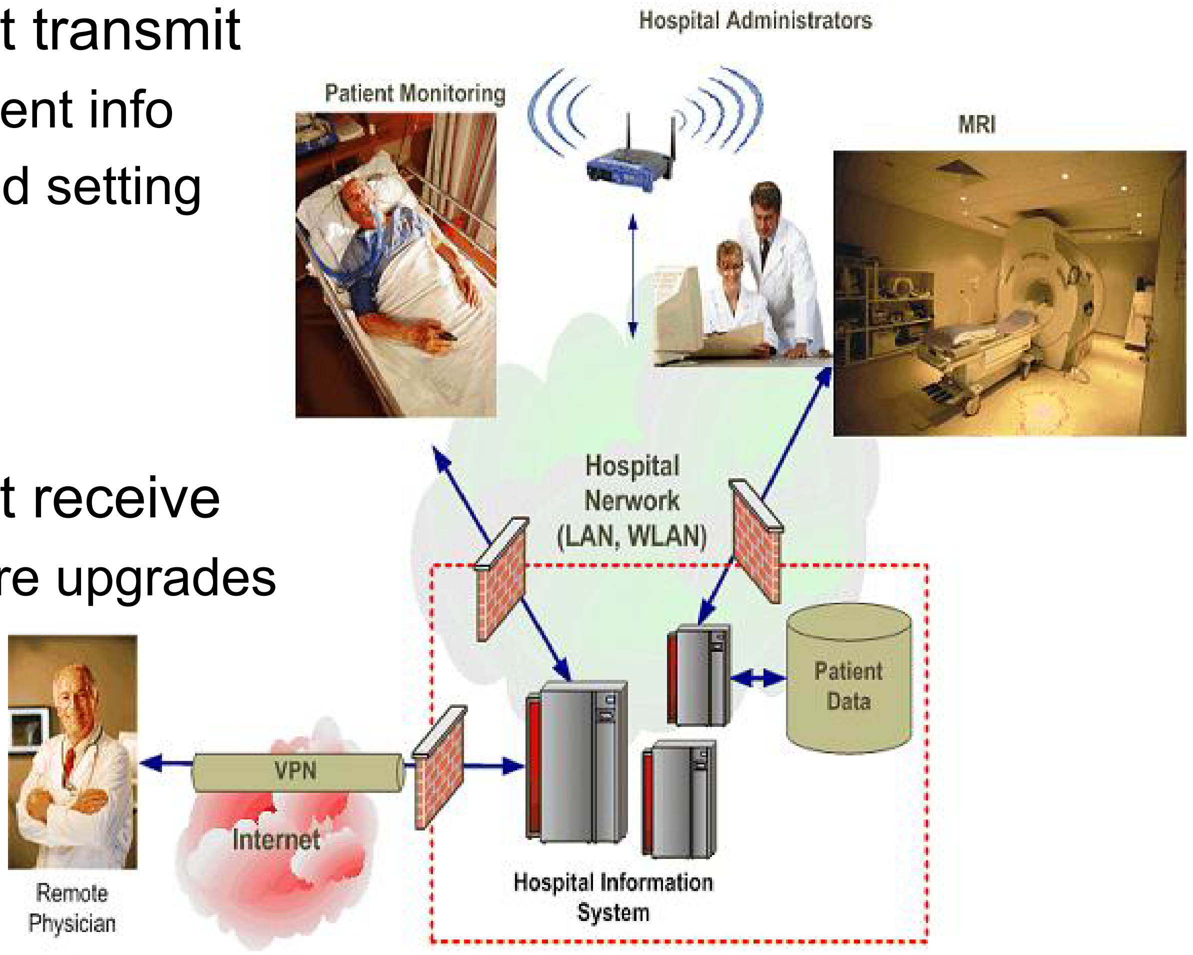
- Examples of devices/systems maintaining and transmitting EPHI



Source: Technology in Medicine, June 2001

Biomedical Devices and IT Systems

- Devices on Internet transmit
  - Location and patient info
  - Current status and setting
  - Diagnostics
  - Error codes
- Devices on Internet receive
  - Software/Firmware upgrades
  - Calibration
  - Diagnostics



HIPAA Security and Biomedical Devices

Historical Perspective

- Biomedical devices utilized at MTFs operated either as stand-alone devices or as networked devices on isolated medical networks
- As such, biomedical devices with unresolved software vulnerabilities posed little or no security threat

HIPAA Security and Biomedical Devices

Current Perspective

- Potential threats
  - Migration of biomedical devices into interconnected networks
    - Subject to vulnerability alerts and patching requirements
  - Unresolved software vulnerabilities due to FDA regulations

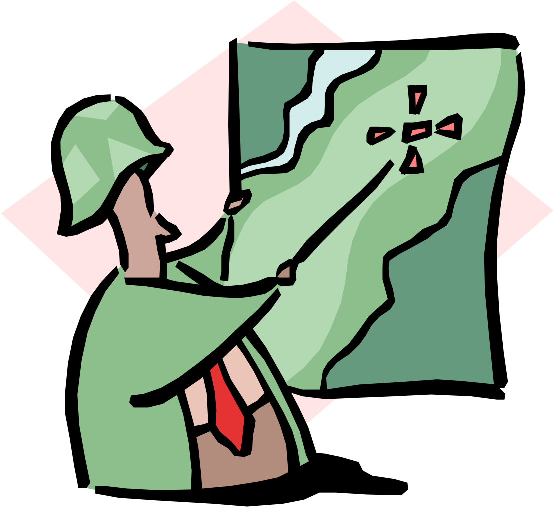
HIPAA Security and Biomedical Devices

Security Risks (1 of 2)

- Biomedical devices
  - Frequently store EPHI, and therefore, must be considered when implementing a comprehensive IT security program
  - Designated and operated as special purpose computers
  - More features are being automated and increasing amounts of PHI is being collected, analyzed, and stored
  - Growing integration and interconnection of different biomedical devices and IT systems where EPHI is being exchanged

Security Risks (2 of 2)

- Approximately 7 software security vulnerabilities are identified each day (Symantec Corporation)
  - Blended threats continue to constitute the most frequently reported threat
    - Combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack



Primary Issue

- FDA requires vendors of medical devices to evaluate the impact of software changes on a medical device’s safety and effectiveness before installing a security patch or upgrade
  - Vendors do not include this type of repair and testing in standard maintenance agreement
  - Evaluation entails unanticipated costs and effort
    - Most computerized medical devices are non-compliant with these FDA requirements

Impact: Organization

- **Risk assessment**
  - MTFs must evaluate the threat to and from biomedical devices in the context of their wider approach to risk management
- **Equipment lifecycle management**
  - Security requirements must be included in contracts or Memorandums of Understanding/Agreement
  - Evaluation and remediation of vulnerabilities must be conducted before the installation of devices on the network
- **Contracts**
  - Must accommodate need for security upgrades to relevant equipment as appropriate and affordable

HIPAA Security and Biomedical Devices

Impact: Architecture

- Multiple, overlapping controls must be developed to support Defense-in-Depth
- Biomedical devices that acquire, distribute, display and archive medical information should be placed on their own physical or virtual segment of the network
- Precise configuration of the medical enclave depends on architectural rules of the wider network

HIPAA Security and Biomedical Devices

Recommendations (1 of 2)

- Share information on solutions amongst your peers
  - The impact is obvious – the more you share amongst your peers, the more time and resources you save
  - Information sharing should not be limited to individual Services but across the MHS

HIPAA Security and Biomedical Devices

Recommendations (2 of 2)

- Develop new requirements in vendor maintenance contracts to cover vulnerability alerts
  - Future contracts should require patches as a component of maintenance
  - Sit down with your vendor and agree on an approach to patching biomedical devices.
- **NOTE:** Precedence for vendors to accept this responsibility has not been established – this is especially true with legacy systems

Community Efforts to Address Issues

- Healthcare Information and Management Systems Society (HIMSS)
  - Biomedical Device Security Taskforce
- National Electrical Manufactures Association (NEMA)
  - Joint Committee on Privacy and Security
- NIST/WEDI/URAC
  - Biomedical Device Security Workgroup
- DoD
  - Biomedical Device Security Committee

HIPAA Security and Biomedical Devices

Summary

- You should now be able to:
  - Describe the relationship between HIPAA security and biomedical devices
  - Detail the risks of using biomedical devices
  - Identify approaches for minimizing these vulnerabilities

Virtual Private Networks (VPN)

Agenda

- HIPAA and VPNs
- Background on MHS VPN Program
- MHS Network Architecture

Training Objectives

- Upon completion of this course, you should be able to:
  - Identify what a VPN is and how it works
  - Describe how HIPAA affects VPNs
  - Illustrate the background of the MHS VPN Program
  - Describe the current status of VPNs within the MHS

HIPAA and VPNs

HIPAA and VPNs

Objectives

- Upon completion of this module, you should be able to:
  - Describe VPNs and how they work
  - Identify the specific HIPAA Security requirements related to VPNs

HIPAA and VPNs

What is a VPN?

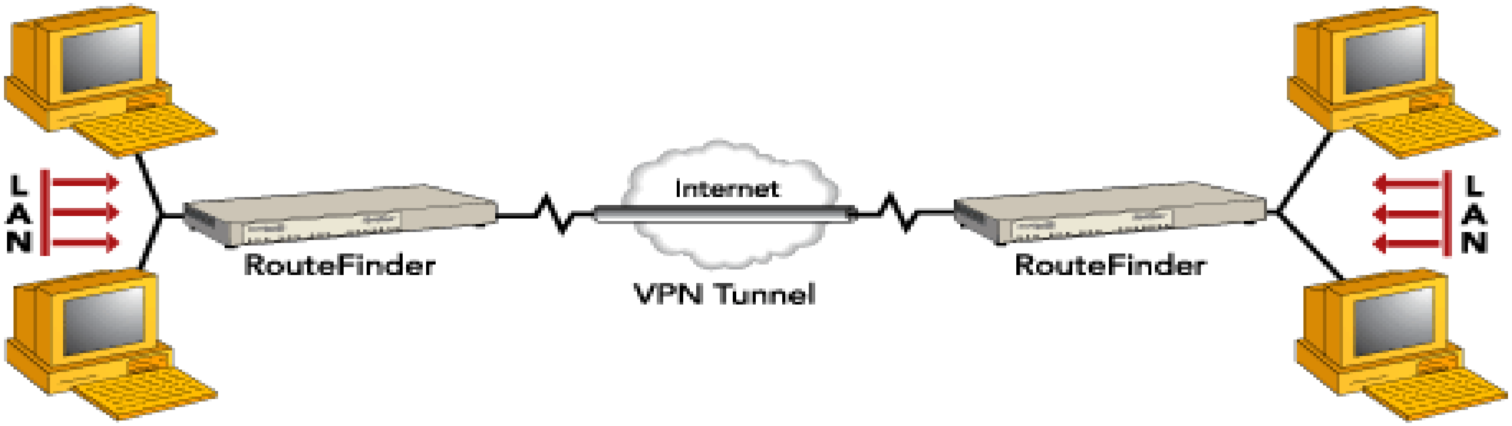
- Virtual Private Network (VPN)
- Distributed collection of networks or systems that are interconnected via a public network (i.e., NIPRNet or the Internet)
  - Secure
  - Tunneled across public network
- Protection for communications through the use of encryption

Source: MHS Information Assurance Policy/Guidance Manual

HIPAA and VPNs

How does a VPN work? (1 of 2)

- Tunneling
  - Used to carry data over the Internet/NIPRNet
  - Sending encrypted packets to a remote server or router over the Internet/NIPRNet. The path through which the packets travel is called a tunnel



Source: Multi-Tech Systems, 2004

HIPAA and VPNs

How does a VPN work? (2 of 2)

- Both the tunnel client and the tunnel server must be using the same tunneling protocol in order to establish a tunnel
- Two VPN tunnels employed within the MHS VPN architecture
  - Internet Key Exchange (IKE)
  - Secure Key Interchange Protocol (SKIP)

HIPAA and VPNs

DoD and Federal Requirements

- Existing DoD requirements and Federal Laws require the protection of sensitive information at-rest and in-transport between DoD Medical Sites
  - DoDI 8500.2
  - CHCS II Command, Control, Communications and Computers Intelligence Support Plan (C4ISP) - Firewall and encryption capability required for all MHS Community of Interest (COI) connected MTFs and Clinics
  - Joint Medical Information Systems Office (JMISO) Draft Policy on Encryption
  - Health Insurance Portability and Accountability Act (HIPAA)

HIPAA and VPNs

HIPAA Security Rule Requirements

- Transmission Security (§164.312(e)(1))
  - Implementation of technical security mechanisms to prevent unauthorized access to PHI that is being transmitted over an electronic communications network
- Encryption (§164.312(e)(2)(ii))
  - Implementation of a mechanism to encrypt EPHI whenever deemed appropriate

HIPAA and VPNs

Implications of HIPAA for VPNs

- Tunnel mode VPNs provide compliance with portions of the HIPAA Security Rule
  - Establish a secure connection between MHS sites
  - Prevent unauthorized access to PHI that is being transmitted
  - Encrypting information transmitted between MHS sites
- **Note**: Does not provide encryption of data at rest but does provide a level of protection of that data

HIPAA and VPNs

Summary

- You should now be able to:
  - Describe VPNs and how they work
  - Identify the specific HIPAA Security requirements related to VPNs

Background on MHS VPN Program

Background on MHS VPN Program

Objectives

- Upon completion of this module, you should be able to:
  - Describe the original deployment for network protection
  - Identify the activities that have occurred to improve that program

Background on MHS VPN Program

Starting Point

- Approximately 250+ MHS facilities - require some level of protection to fully comply with DoD and Federal requirements
- TIMPO IA Program
  - Underlying Standards based infrastructure to protect MHS
    - Networks
    - Sites
    - Data

…from loss or disclosure both at-rest and in-transport. **

** Protection of Air Force Site MTFs provided under Combat Information Transport System (CITS) Program

Background on MHS VPN Program

Large Network Protection (NP) Suites

- Large NP Suites
  - Initial fielding completed in 2000
  - Provide required “defense-in-depth” capabilities at (65) Army and Navy CHCS Host and Major Satellite (Parent DMIS) Sites
  - Current Large Suites are managed by Local Site Staff with support provided by TIMPO/SPAWAR
- VPN activation delayed due to persistent problems with Avaya VPN hardware and software
  - Hardware replaced in 2001
  - Limited activation at select Army and AF MHS Sites

Background on MHS VPN Program

VPN Management

- VPN Management
  - Tasked to DISA-San Antonio for domain/device operations and management
  - Transitioned to DISA Montgomery in mid-2002
- VPN Working Group
  - Formed March 2003
  - Provide focal point for Joint TIMPO/Services/DISA support for VPN activation and operations
  - Control and coordinate changes to the domain via Management Information – Coordination Control Board (MI-CCB)

Background on MHS VPN Program

Major Milestones (1 of 3)

- Major completion milestones in 2003:
  - Activation of existing VPN Devices at 65 Sites
    - Completed May 31
  - Encryption of TOL, CHCS DEERS, SIDR/SADR, Lab Interop
    - Completed July 30
  - Activation of AF and VA VPN Gateways
  - Addition of (14) AF Sites to MHS VPN without access to the AF VPN Gateway
    - Completed Oct 14, 2003 to support HIPAA mandate for protection of eligibility and claims data.

Background on MHS VPN Program

Major Milestones (2 of 3)

- June 2003
  - DISA proposed for replacement of Avaya VPN with Next Generation Encryption Solution (N-GES) using NetScreen VPN hardware and Global Pro Management Suite
- July 2003
  - DISA Project task for a three (3) Phase deployment approach approved by TIMPO Program Manager

Background on MHS VPN Program

Major Milestones (3 of 3)

- August 2003
  - Joint NP Working Group (TIMPO/DISA/Services) Off-Site
  - Held at SPAWAR Systems Center Charleston
  - Reviewed objectives and plans for 2004 NP Program. Topics included:
    - Technology Refresh Plan for Large NP Suites
    - DISA N-GES Avaya VPN Replacement Program
    - CHCS II-COI Network Security Requirements
    - Proposed MHS NP Architecture (4-Tier Model) supporting extension of network security to Satellite and Remote Clinics
    - Small Suite Program, scope and implementation requirements

Background on MHS VPN Program

Summary

- You should now be able to:
  - Describe the original deployment for network protection
  - Identify the activities that have occurred to improve that program

MHS VPN Architecture

MHS VPN Architecture

Objectives

- Upon completion of this module, you should be able to:
  - – Describe the current MHS VPN architecture
  - – Describe the target MHS VPN architecture
  - – Detail current deployment status of VPN devices

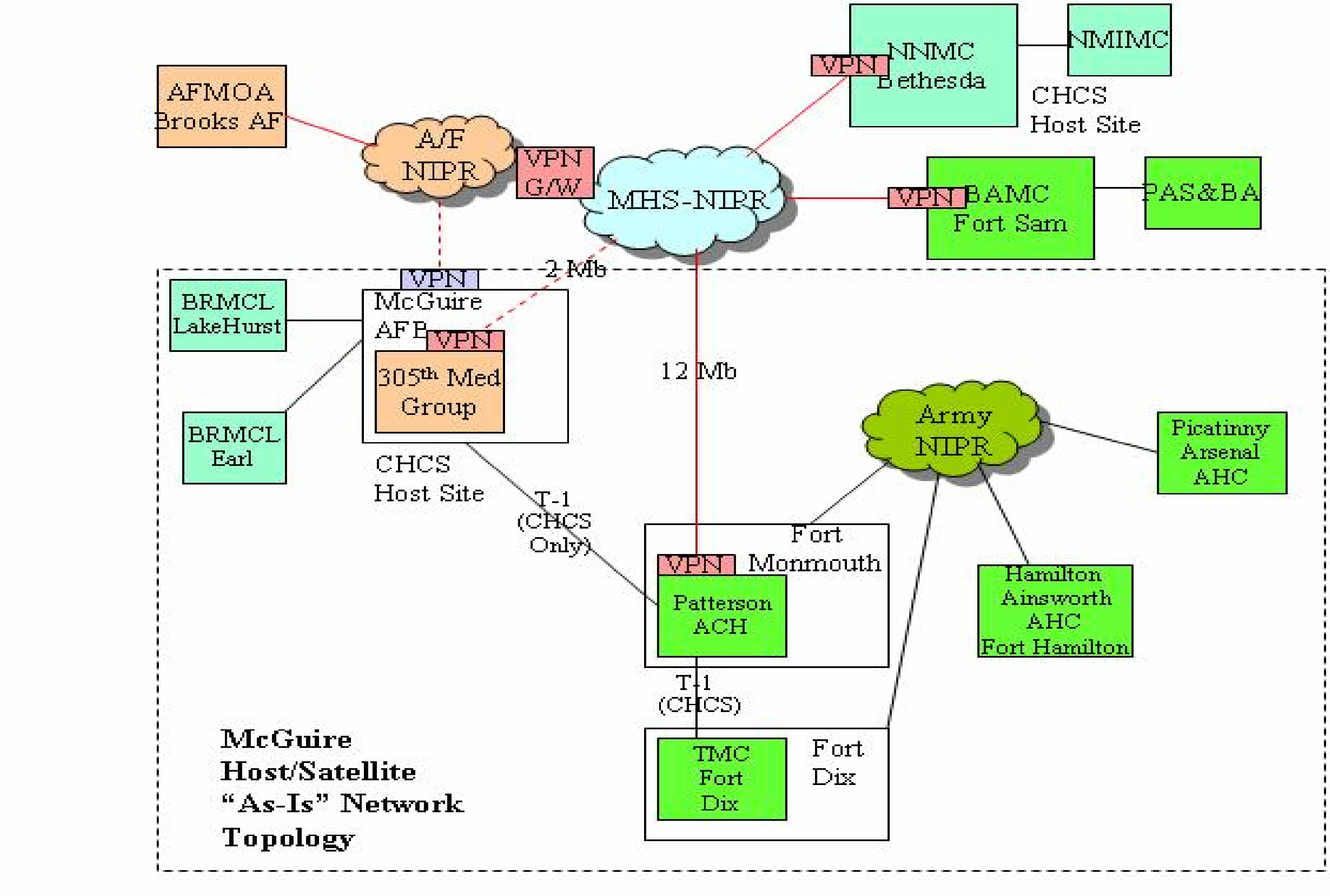
MHS VPN Architecture

Challenges

- 250+ MHS facilities
  - Not all facilities addressed under the TIMPO IA program
  - All require some level of protection to fully comply with regulations
- Existing Large NP Suites protect data
  - At CHCS Host/Parent DMIS MTFs
  - At satellites connected behind the Parent Site’s firewall

MHS VPN Architecture

CHCS Host-Satellite Architecture

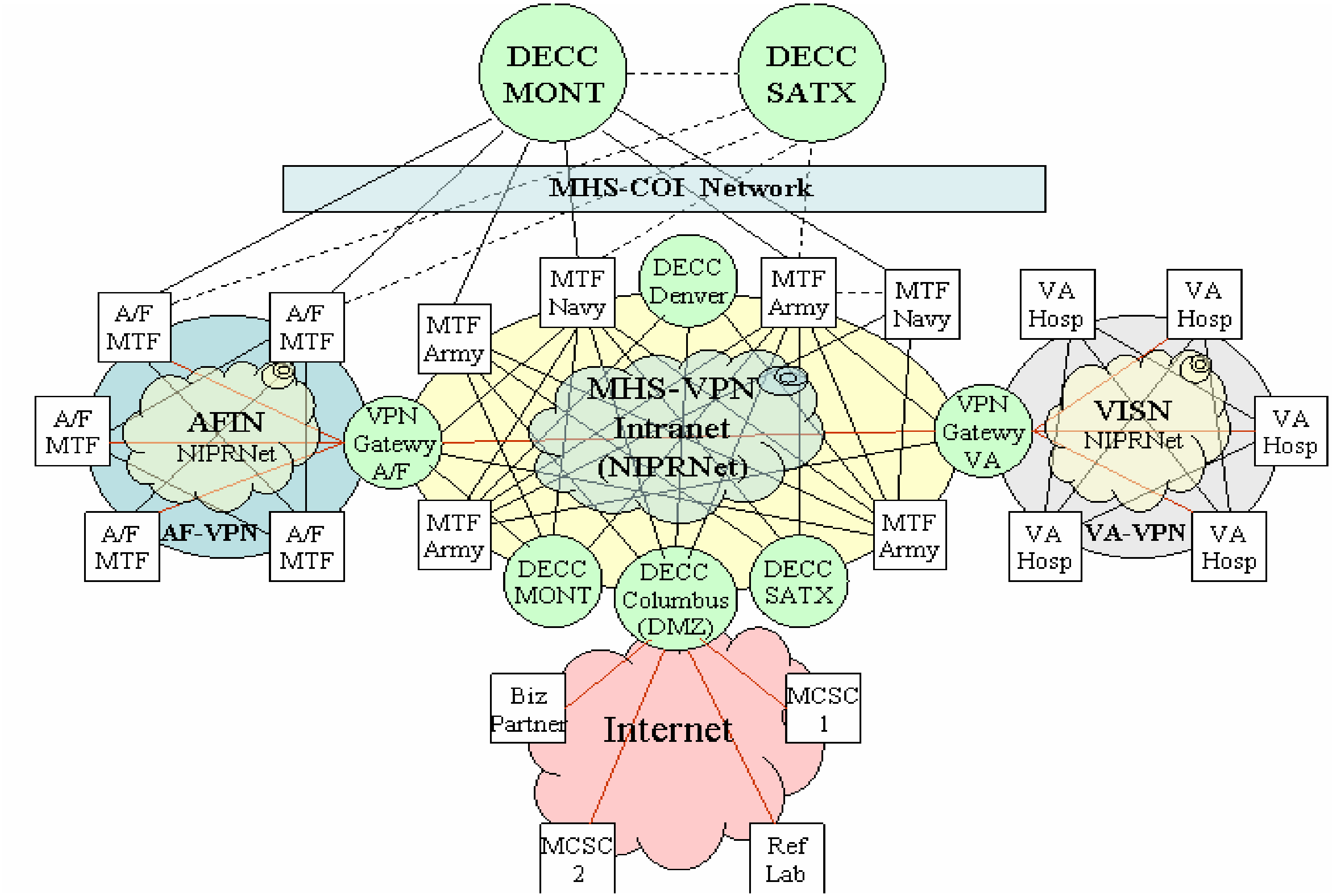


MHS VPN Architecture

Challenges(cont.)

- MHS-VPN ‘Mesh’ protects data in-transport between MTFs, DISA DECCs, and existing VPN Gateways (AF, VA, Business to Business (B2B))
  - Data transport between Host/Parent MTFs and Satellites remain mostly unprotected
  - Roughly 30% of Satellites have no direct connection to the Parent MTF

MHS VPN Domain Architecture



MHS VPN Architecture

Solution - MHS Small Suites Program

- Four (4) Tier Architecture
  - Basis for projecting NP requirements
  - Based on application data flow and connectivity between DISA DECCS (Tier 1), Host/Parent Sites (Tier 2), and Satellite Clinics (Tier 3 and 4)

Small Suites	**Tier 3**	**Tier 4**	**Total**
Service			
Army	42	78	120
Navy	38	92	130
Total	80	170	250

Source: TIMPO, 2004

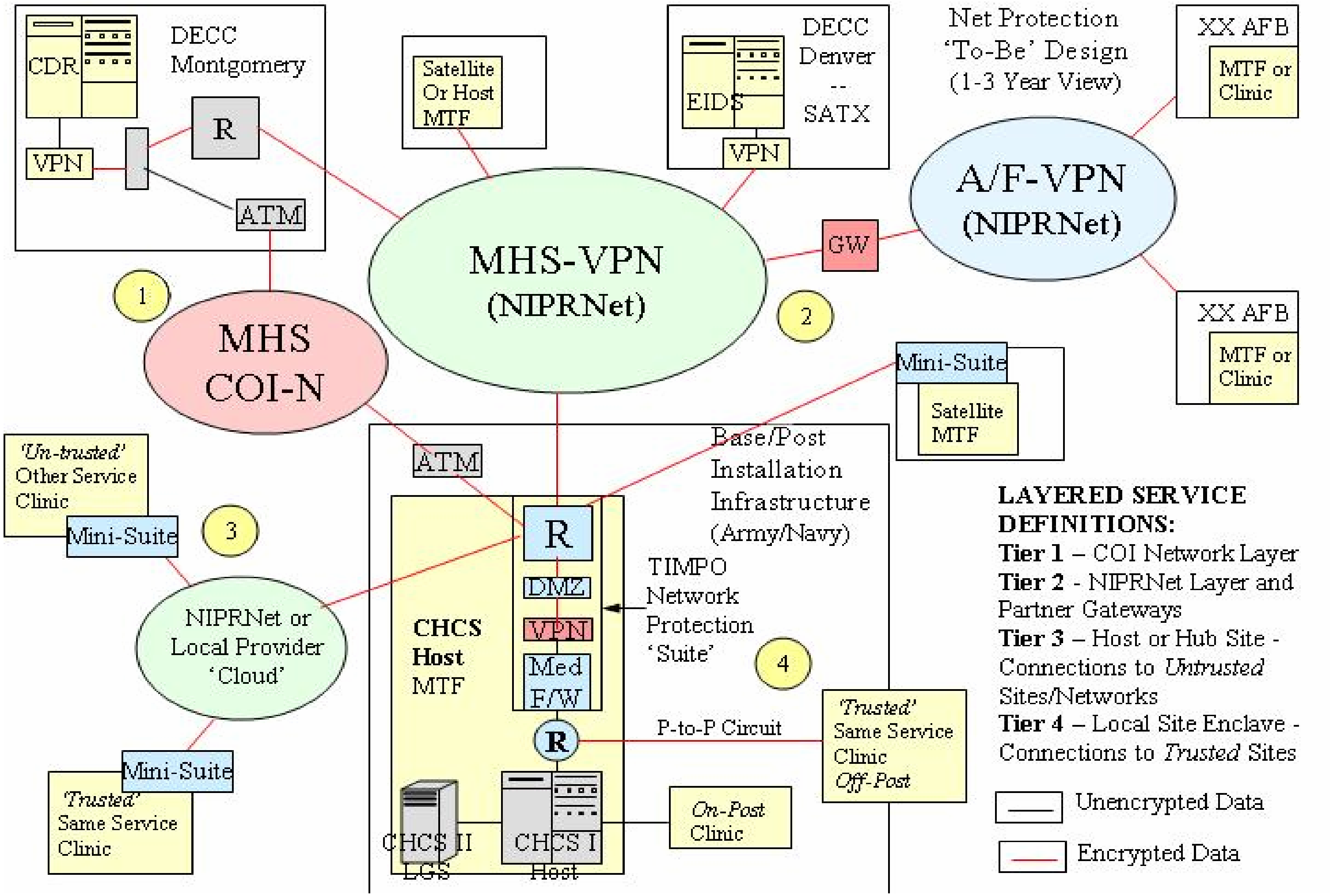
MHS VPN Architecture

Which Applications are Included?

- Enterprise Applications that are encrypted
  - CHCS II
  - DBSS
  - EWRAS/NAS
  - TOL
  - PCMBN/CCQAS
  - Lab Interoperability
  - SIDR/SADR
  - X12 DEERS
  - PHCS
  - SNPMIS
  - MRTR2 Records Archives

MHS VPN Architecture

MHS Target NP Architecture (1 of 3)



LAYERED SERVICE DEFINITIONS:

Tier 1 – COI Network Layer

Tier 2 - NIPRNet Layer and Partner Gateways

Tier 3 – Host or Hub Site - Connections to *Untrusted* Sites/Networks

Tier 4 – Local Site Enclave - Connections to *Trusted* Sites

Unencrypted Data

Encrypted Data

MHS VPN Architecture

MHS Target NP Architecture (2 of 3)

- **Tier 1 Site** – DISA Defense Enterprise Computing Centers (DECC)

- **Tier 2 Site** – CHCS Host or Parent DMIS Site using DATMS-U or COI for communication with other MHS Sites
  - Requires full “layered defense” Network Protection (NP) Suite to secure data at-rest and in-transport

MHS VPN Architecture

MHS Target NP Architecture (3 of 3)

- **Tier 3 Site** – Satellite Clinic using a Shared Layer 3 Network (NIPRNet, Regional MAN), COI Network, or a commercial T-1, connected outside the Host facility NP Suite, to communicate with Parent Tier 2 or Tier 1 Site
  - Requires "Mini-suite" to secure data

- **Tier 4 Site** – Off-Post Clinic that has one or more commercial T-1 circuits terminating behind the Parent Tier 2 Site NP Suite
  - Requires VPN only to secure data in-transport

MHS VPN Architecture

Deployment Status

- **Key Terminology:**
  - **Staged** sites are sites that are currently being worked on or are under review.
  - **Inactive** sites are sites that require either concurrence from the service or a solution is being created.

MHS VPN Architecture

VPN and Avaya VSU Device Status

Service	Operational	Down	Staged	Inactive	Totals
	Sites	Sites	Sites	Sites	All Sites
Air Force with Avaya VSUs	19	0	0	0	19
Air Force in the AF Gateway (*)	46	0	0	0	46
Army	42	0	0	6	48
Navy	26	0	0	1	27
MHS Other	19	0	0	0	19
US Coast Guard, Martinsburg, WVA	1	0	0	0	1
New Totals	153	0	0	7	160

Report is as of 6/17/2004

MHS VPN Architecture

VPN and Netscreen Device Status

Service	Operational	Down	Staged	Inactive	Totals
	Sites	Sites	Sites	Sites	All Sites
Air Force with Netscreens	10	0	0	71	81
Air Force in the AF Gateway (*)	0	0	0	44	44
Army	27	0	0	27	54
Navy	23	0	0	32	55
Managed Care Support Contractors	13	0	0	3	16
MHS Other	14	0	0	3	17
US Coast Guard, Martinsburg, WVA	0	0	0	1	1
National Guard	1	0	0	0	1
New Totals	88	0	0	181	269

Report is as of 6/17/2004

MHS VPN Architecture

Status of Projects Using the VPN

Service	Operational	Down	Staged	Planning	Totals
	Site Instances	Site Instances	Site Instances	Site Instances	Site Instances
Tricare On-Line (**) (***)	103	0	0	0	103
EWRAS/ NAS (**) (***)	103	0	0	0	103
CCQAS/ PCMBN (***)	103	0	0	0	103
DBSS	16	0	0	0	16
CHCS II (***)	66	0	0	0	66
Lab Interoperability (***)	36	0	0	0	36
EI/DS HL7 Transfers	91	0	0	0	91
EI/DS SIDR/SADR Transfers	97	0	0	0	97
DEERS (HIPAA X12) (****)	109	0	0	1	110
PHCA	18	0	0	0	18
SNPMIS	20	0	0	18	37
MRTR^2	103	0	0	0	103
New Totals (#)	865	0	0	19	883

(**) Still working on connectivity issues between MCSC and TOL

(***) Expecting World Wide deployment within the next year.

(****) Pending circuit activation for the USNS Comfort.

(#) Totals Include known Host, Satellite, MCSCs, and Other sites using the VPN.

Report is as of 6/17/2004

MHS VPN Architecture

VPN Statistics

	Avaya	Netscreen
Number of VPN Devices	153	88
Number of Tunnel Endpoints	242	88
Number of VPN Objects	98	N/A
Number of VPN Tunnels	29,161	3,828

Report is as of 6/17/2004

MHS VPN Architecture

Summary

- You should now be able to:
  - Describe the current MHS VPN architecture
  - Describe the target MHS VPN architecture
  - Detail current deployment status of VPN devices

VPN Summary

- You should now be able to:
  - Describe how HIPAA affects VPNs
  - Identify what a VPN is and how it works
  - Describe the current status of VPNs within the MHS

Resources

Network Protection Working Group (1 of 6)

- TIMPO members

Name	Office Phone	E-Mail Address
Tom Hines	(703) 399-2214	tom.hines@tma.osd.mil
Glenn Marshall	(703) 399-2214	glenn.marshall@tma.osd.mil
Rob Brown	(703) 399-2231	robert.brown@tma.osd.mil

Resources

Network Protection Working Group (2 of 6)

- SPAWAR members

Name	Office Phone	E-Mail Address
Don Oswalt	(843) 218-4670	donald.oswalt@spawar.navy.mil
Cal Stephens	(843) 218-4370	charles.stephans@spawar.navy.mil
MHS-IA Help Desk	(843) 218-5210 or 5212	

Resources
Network Protection Working Group (3 of 6)

- Air Force members

Name	Office Phone	E-Mail Address
Major Drexel DeFord	(703) 681-6166	Drexel.DeFord@pentagon.af.mil
Major Mike Brummett	(703) 681-6167	Michael.Brummett@pentagon.af.mil
Richard Binkley	(210) 536-4034	richard.binkley@brooks.af.mil
Richard Trice	(210) 536-3981	richard.trice@brooks.af.mil

Resources
Network Protection Working Group (4 of 6)

- Army member

Name	Office Phone	E-Mail Address
Anthony Giljum	(210) 643-7906	anthony.giljum@cen.amedd.army.mil

- Navy members

Name	Office Phone	E-Mail Address
Robert E. Lee	(301) 319-	relee@us.med.navy.mil
Dale Edgeington	(301) 319-1257	deedgeington@us.med.navy.mil

Network Protection Working Group (5 of 6)

- DISA HQ members

Name	Office Phone	E-Mail Address
Andrew Herns	(703) 681-1339	hernsa@ncr.disa.mi
Dave Rook	(703) 681-2205	rookd@ncr.disa.mil
Ray Brittner	(303) 438-7028	brittnerr@netcsc.com

Resources

Network Protection Working Group (6 of 6)

- DISA Montgomery Members

Name	Office Phone	E-Mail Address
DISA-MHS Help Desk	(334) 416-6666	vpnteam@mont.disa.mil
Ken Tuck	(334) 416-3650	tuckk@mont.disa.mil
Hugh Schmidt	(334) 416-1682	schmidth@mont.disa.mil

Resources

- MHS Information Assurance Policy/Guidance Manual, February 12, 2003
- https://rimr.tatrc.org/
- http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- hipaamail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- HIMSS - http://www.himss.org/
- NEMA - http://www.nema.org/
- NIST/WEDI/URAC - http://www.URAC.org
- Service HIPAA representatives

Please fill out your critique

Thanks!